White Paper

Governance-Based Access Control (GBAC): Enabling improved information sharing that meets compliance requirements

TABLE OF CONTENTS

While information sharing delivers numerous benefits, organizations have grown frustrated with finding the best approach to ensuring that this information is properly collected, shared and managed. Traditional access control models no longer meet the broad and complex requirements of information sharing within and outside of organizational boundaries. As government regulations and customer and citizen demands continue to increase, organizations must find a way to implement a more sophisticated access control scheme. GBAC is one viable solution that helps organizations facilitate robust information sharing, while properly managing and mitigating the inherent risks.

Introduction

Never before has it been easier to share information. Information sharing allows government and commercial organizations to enhance their value, from enabling the development of "seamless service delivery" to citizens and customers, to helping coordinate response capabilities against criminal activities and terrorist threats.

Yet information sharing also leads to precarious situations. For instance, according to the Computer Security Institute, data theft from external and internal sources grew at a rate of more than 650 percent between 2001 and 2004, demonstrating that the ability to electronically transmit information from one organization to another presents risks, such as the abuse and misuse of confidential, personal, medical and financial information.

While the private sector is grappling with recent well-publicized incidents involving breaches of sensitive customer information, the public sector in large part has been operating without specific regard to how information sharing arrangements could compromise their organizations, or more importantly, the rights of citizens. As the public becomes more aware of these incidents and arrangements, they are calling for stronger restrictions and greater transparency regarding how customer and citizen information is protected, managed and used.

Recognizing the value of information sharing—while at the same time preventing misuse and privacy breaches—legislatures around the world are increasingly requiring public- and private-sector organizations to comply with a host of new measures aimed at setting boundaries on when and how information should be collected, shared, managed and disposed of, and under which circumstances. Examples of some of these countries' measures include:

- **Australia**—Federal Privacy Act
- **Canada**—Personal Information Protection of Electronic Documents Act (PIPEDA), Federal Privacy Act, National Archives Act, Access to Information Act, Security of Information Act
- **Europe**—European Data Protection Directive
- **United States**—Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, California Security Breach Notification Law, Fair Credit Reporting Act, Health Insurance Portability Accountability Act (HIPAA), Freedom of Information Act (FOIA), U.S. Patriot Act

To help organizations benefit from information sharing, while addressing its inherent challenges, this paper discusses how information sharing may be viewed and approached, in part, as an issue of access control. While traditional access control models do not meet the broad and complex requirements of interorganizational information sharing, a new, more sophisticated access control scheme called Governance-Based Access Control (GBAC) helps address today's broad and complex access requirements. GBAC provides organizations with a fundamental enabler for information sharing across organizational and jurisdictional boundaries, while taking into account the many requirements imposed by the multiplicity of governing legislation. The paper also briefly discusses how GBAC may be used to enable shared service delivery models and to increase transparency and accountability within the emerging environment of open, interconnected and inter-jurisdictional organizations.

New challenges for access control

Rigorous access control of information holdings has always been a priority for organizations. In fact, it's been the cornerstone of many security policies dealing with the protection of information asset holdings. In the past, when information was kept strictly inside the organization, the traditional approaches to access control worked extremely well. However, with organizations now required to increasingly share information to outside sources, these traditional access control models are no longer sufficient.

For government agencies, private-sector companies and non-profit organizations, realizing the benefits of information sharing while complying effectively with the restrictions imposed by privacy legislation is a daunting task. Most organizations still rely upon traditional access control models that were never intended to deal with the security demands of sharing information beyond the originating organization. To successfully cope with the accountabilities and risks inherent within this new environment, organizations must reconsider how they categorize and classify their information assets and how they determine who has a right to access each asset.

Presently, most organizations consider the use and protection of their information holdings using only two factors: the system in which it is housed and its security classification. Internal access control and data-sharing security models reflect this reality by relying on the following commonly used models.

- **Identity-Based Access Control** permits access to data based upon the users or owners of the data. Also known as Discretionary Access Control (DAC), this model requires explicit knowledge beforehand of all the users who may potentially require access to data.
- **Rules-Based Access Control** permits access to data based upon formally defined security levels assigned to information and the clearance levels assigned to individuals and processes. Also known as Mandatory Access Control (MAC), this model addresses only security and protection requirements and not "need-to-know" or privacy-related requirements.
- **Role-Based Access Control (RBAC)** permits access to data based upon an organizational role, such as a clerk or investigator, which has been assigned to an individual within the organization. RBAC is effective in reducing administrative burden by associating permissions based upon “need to know” roles instead of individuals, and is more efficient at handling operational changes by administering permissions of organizational roles and assigning these roles to individual people.

These models of access control operate on the predominant assumptions that only a single organization requires access to information, information is only accessed by internal users of the organization, and everyone is subject to or must be compliant with a single authority. However, as businesses, governments and societies become increasingly interconnected and as information is increasingly shared across organizational and jurisdictional boundaries, these assumptions no longer hold true. As such, the traditional models are no longer sufficient.

Faced with new responsibilities in both sharing and safeguarding information, many organizations are paralyzed by fear and indecision. They don’t understand the governance structure of their information or their responsibilities in sharing and protecting that information. They hesitate because they are struggling with such issues as:

- The possible legal exposure a decision might incur for the organization
- The risk of data being used inappropriately, such as for data matching or linkage
- The potential loss of control or power over their information assets
- The absence of a clear consensus within the organization on the true value or purpose of the information at hand

The result? Valuable information remains locked in organizational silos and is difficult—often impossible—to share.

The evolution of access control

No one can deny the new reality of an increasingly interconnected world. To effectively operate, all organizations must share confidential or personal information; however, they must also remain accountable for ensuring that this information is effectively safeguarded and, once shared, properly used. Government agencies and companies that fail to abide by the laws that dictate these standards can experience real consequences, including damage to their reputation, legal liability and difficulty in getting citizens, customers or partner organizations to disclose crucial information.

So how do organizations effectively share information, comply with so many different legal demands, and yet somehow mitigate the risk of allowing sensitive information to leave the domain of their own networks and organizations? Fortunately, these needs can be addressed—and information sharing can still be viewed—as an access control problem that has evolved to meet the following new assumptions:

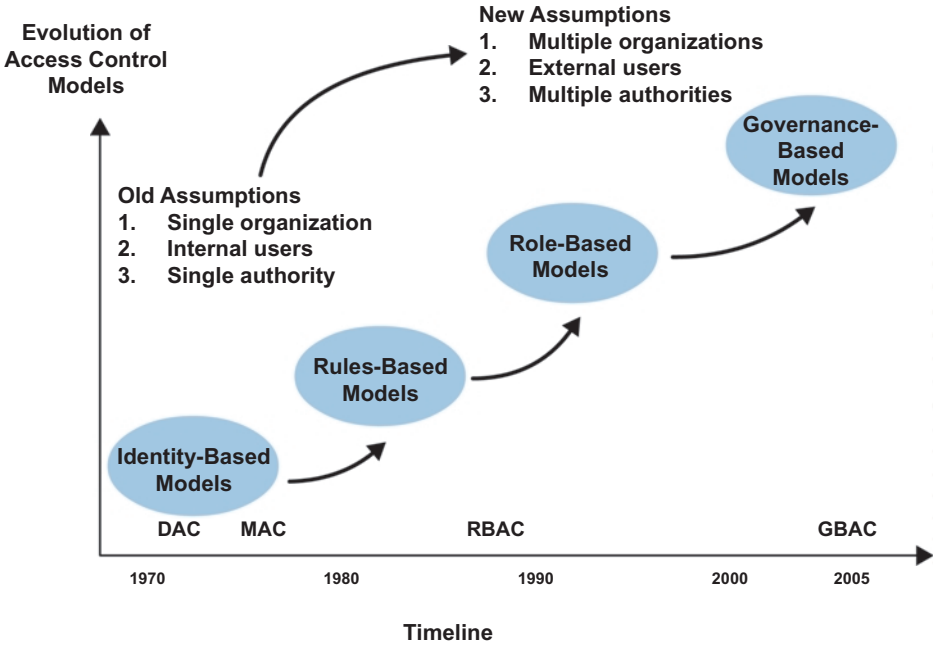
- Many organizations may require access to information
- Information may be accessed by, or shared with, external users
- Everyone may be subject to compliance with multiple authorities and jurisdictions

An emerging model based on governance can effectively address these new assumptions. That model is called Governance-Based Access Control (GBAC).

An improved method: The GBAC model

GBAC is an innovative and evolutionary extension of the traditional access control models. Figure 1 illustrates how access control models have evolved over time.

Figure 1: Evolution of Access Control



As the figure illustrates, GBAC is the most recent access control model to emerge. GBAC builds upon the traditional access control models of the last 30 years, and addresses new assumptions for access control that simply did not exist when information was shared and stored in separate information silos for internal use only. GBAC enables organizations to address the new requirements of sharing information beyond their boundaries, while embracing and enhancing the traditional access control models by maintaining security, privacy and the compliant use of shared information.

GBAC is the most recent access control model to emerge. It builds upon traditional models to address new requirements for access control. It classifies and accesses information asset holdings by directly linking them back to specific legal measures that mandate their use, and takes into account the "why" behind the information and the "who" required to access the information.

The fundamental premise of GBAC is simple—when an organization collects, uses, manages or shares personal and sensitive information, the resulting information asset, throughout its entire lifecycle, must be governed by the relevant legislation to which the organization is accountable and must comply. At its essence, GBAC is a method of classifying and accessing information asset holdings by directly linking them back to the specific legal measures that mandate their collection, dissemination, protection and disposition.

GBAC considers the larger issue of why information is being held in the first place, and takes into account that multiple authorities may be required to determine an access control or information sharing decision.

Using GBAC, access permission rules can be specified and applied against any information asset defined by the organization—be it a single customer database record, an entire database collection or an individual document or e-mail. These rules can be rigorously enforced according to key governance questions. The key governance questions can be answered by determining the following six attributes of each defined information asset.

1. **Jurisdiction**. What jurisdiction is originally, currently or ultimately responsible for this information asset?
2. **Collection authority**. Under what specific legislative authority, regulation or governing policy was this information asset collected and used, including subsequent use?
3. **Collection purpose**. What was the reason, purpose or business process behind the collection of this information asset?
4. **Security designation**. What is the sensitivity of the information asset or the potential damage its disclosure might cause?
5. **Disclosure authority**. What is the authority that enables this information asset to be disclosed beyond its original authority and/or reason?
6. **Disposition authority**. What is the authority under which the information asset may be disposed?

Because each specific information asset can be tied back to its true and original purpose, GBAC provides a framework for classifying an information asset that reflects its true and original purpose. It also provides a common way to specify rules of governance that may be used to enforce access to information assets irrespective of where they reside, be it on a system or within the organization.

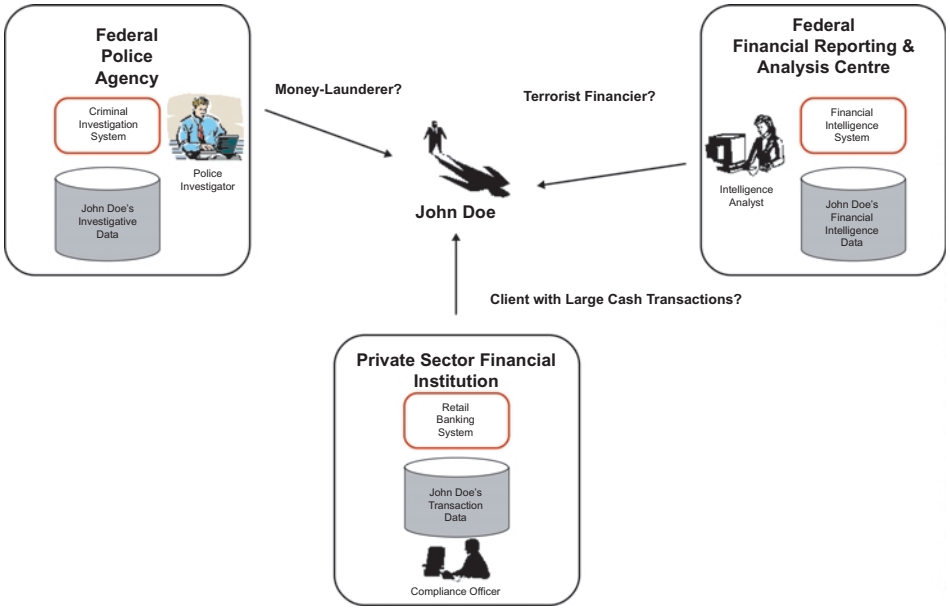
Further, by linking an information asset to its governance structure, organizations are in effect placing a warning label on it, along with an accompanying set of rules stipulating how this asset may be used and under what circumstances. This act removes a major element of risk from the publishing organization by placing specific rules, conditions and responsibilities on the subscribing organization—in a manner analogous to a warning label placed on a consumer product which puts the legal onus on the purchaser to observe the warnings and restrictions on the label.

GBAC in action: An example of how the model works

To help illustrate the GBAC model, consider the following scenario demonstrating how it might work in the real world. Let's say there are three organizations that have dealings with a Canadian citizen named John Doe: a federal police agency, a federal financial reporting and analysis centre, and a private-sector financial institution. John Doe is engaged in money-laundering activities for the purposes of financing a terrorist organization. John Doe has been successful in conducting his illicit activities because, separately, no one has a complete picture of John Doe that would lead to his apprehension.

Figure 2 illustrates the incomplete picture each organization has of John Doe.

Figure 2: Incomplete picture of John Doe



Based upon the information collected and used regarding John Doe, each organization has an incomplete picture. Which of the following is John Doe?

- **A money-launderer**? The police agency investigating John Doe views him as a potential low-risk criminal suspect involved in a money-laundering ring, and is unaware of his terrorist financier status.
- **A terrorist financier**? The analysis centre that has targeted John Doe views him as a potential terrorist financier, and they are unaware of his money-laundering activities.
- **A client with large cash deposits**? The financial institution where John Doe is a banking client views him as a regular customer who deposits large sums of cash, and they are unaware that he is a suspected criminal and intelligence target.

This scenario illustrates how GBAC may be used in conjunction with RBAC. Instead of individuals, there are three roles that require shared information: a police investigator, an intelligence analyst and a compliance officer. These roles can be assigned within each organization to the individuals who require access.

Table 1 details the information collected by each organization, which accesses and uses it according to their role, and demonstrates how the resulting information assets might be classified according to GBAC.

Table 1: Information collected by each organization on John Doe

Federal police agency John Doe is a money-laundering suspect. A police investigator is conducting an investigation and collects evidence pertaining to John Doe. This information is stored as investigative data in the criminal investigation system. The resulting GBAC classification of John Doe's investigative data is as follows: ✓ **Jurisdiction:** Federal ✓ **Collection authority:** Federal Police Act ✓ **Collection reason:** Money-laundering investigation ✓ **Security designation:** Protected C or Protected B ✓ **Disclosure authority:** Federal Privacy Act ✓ **Disposition authority:** National Archives Act
Federal financial reporting and analysis centre John Doe is an intelligence target who may be a threat to national security. An intelligence agent is developing a profile on John Doe, collecting sensitive information designated according to some of Canada's national security rankings as Top Secret, Secret, Protected C or Protected B. The information is stored as intelligence data in the financial intelligence system. The resulting GBAC classification of John Doe's intelligence data is as follows: ✓ **Jurisdiction:** Federal ✓ **Collection authority:** Proceeds of Crime & Terrorist Financing Act ✓ **Collection reason:** Suspicious Financial Transactions ✓ **Security designation:** Top Secret or Protected B ✓ **Disclosure authority:** Privacy Act ✓ **Disposition authority:** National Archives Act
Private-sector financial institution John Doe is a client who has been depositing large sums of cash. This information is collected as transaction data in the retail banking system. To comply with the Proceeds of Crime & Terrorist Financing Act, a compliance officer is identifying large cash deposit transactions greater than $10K as suspicious deposit transactions. The resulting GBAC classification of John Doe's transaction data is as follows: ✓ **Jurisdiction:** Federal ✓ **Collection authority:** Proceeds of Crime & Terrorist Financing Act ✓ **Collection reason:** Standard or suspicious deposit transactions ✓ **Security designation:** Client confidential ✓ **Disclosure authority:** PIPEDA ✓ **Disposition authority:** PIPEDA

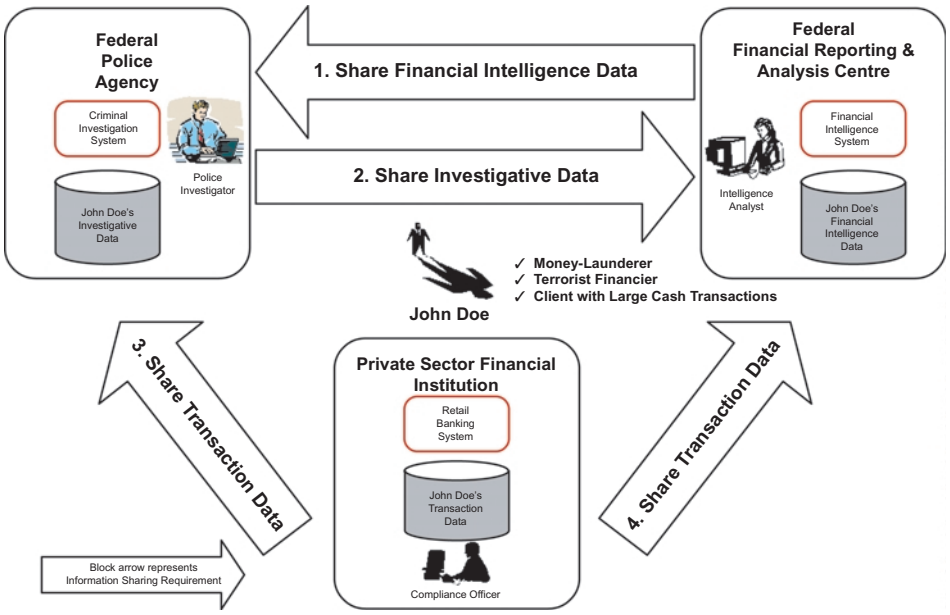
To develop a complete picture of John Doe, these three organizations must share information with one another to bring together the separated facts to determine that John Doe is, in fact, all of the following:

- **A money-launderer** who realizes significant financial proceeds from money-laundering transactions
- **A terrorist financier** who uses these proceeds to finance a known terrorist organization
- **A client with large cash deposits** which are then immediately transferred to a different account

As the example illustrates, GBAC enables the information from three disparate organizations to come together to present a complete picture of John Doe's criminal activities. Through the means of GBAC rules, information-sharing requirements can be associated with the sharing of data to enforce who (or what role) can gain access to certain information.

Figure 3 illustrates the complete picture of John Doe enabled by information sharing among these three organizations.

Figure 3: Complete picture of John Doe enabled by information sharing



In this information-sharing scenario, there are four critical "information-sharing requirements" that enable John Doe's complete picture to emerge. These requirements, along with their benefits and risks, are outlined below.

1. **Share financial intelligence data**—*Requirement:* The federal financial reporting and analysis centre must share financial intelligence data on John Doe to the federal police agency. *Benefit:* Shared information helps the police investigator understand that John Doe is not a low-risk, but rather a high-risk suspect. *Risk:* The centre could share information on John Doe that jeopardizes the police investigation.
2. **Share investigative data**—*Requirement:* The federal police agency must share investigative data on John Doe to the federal financial reporting and analysis centre. *Benefit:* This shared information helps the intelligence analyst build a better profile of John Doe and his money-laundering patterns. *Risk:* The federal police agency could share highly sensitive information of John Doe that could result in injury or loss of life.
3. **Share transaction data**—*Requirement:* The financial institution must share transaction data to the federal police agency on John Doe, who is under police investigation. *Benefit:* This shared information helps the police investigator gather more complete investigative data on John Doe, resulting in more criminal charges and more evidence for eventual prosecution. *Risk:* The financial institution could share information on John Doe that is not salient to the police investigation, thereby compromising his privacy rights.
4. **Share transaction data**—*Requirement:* The financial institution must identify and share transaction data to the federal financial reporting and analysis centre on large cash deposits to comply with the Proceeds of Crime & Terrorist Financing Act. *Benefit:* In addition to assuring that compliance requirements are being met, this information helps the intelligence analyst more quickly identify new intelligence targets. *Risk:* The financial institution could share information of all its clients' deposit transactions, compromising customer privacy rights and the institution's reputation.

GBAC can enable these information-sharing requirements by means of GBAC rules, which directly correspond to the four information-sharing requirements in the above scenario. These rules can be used to enforce who (or what role) can gain access to certain information contained within critical information systems regardless of whether they are from inside or outside of the organization. Figure 4 illustrates the scenario's GBAC rules.

Figure 4: Information sharing enabled by GBAC rules

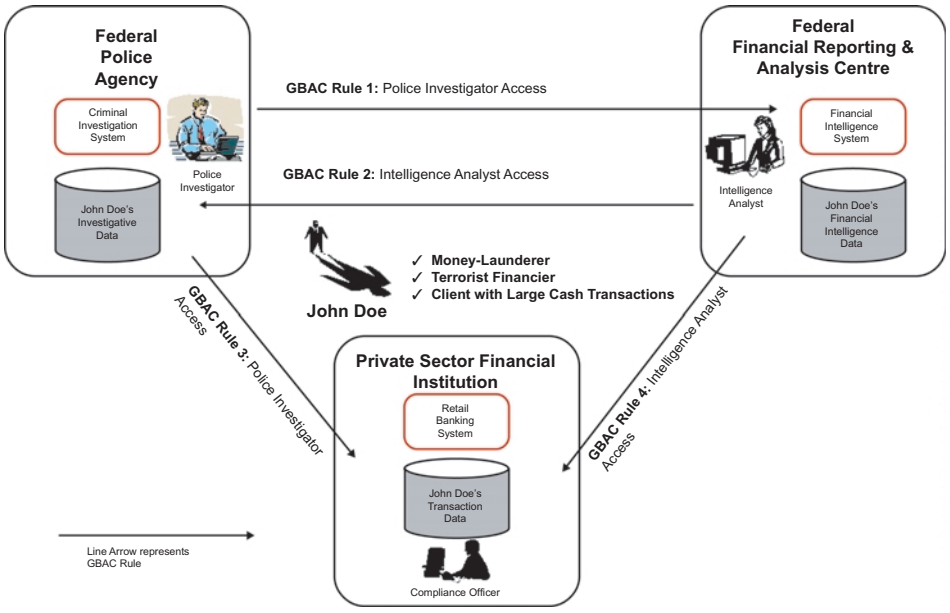


Table 2 provides detail on each GBAC rule corresponding to the information-sharing requirements.

Table 2: GBAC rules

GBAC rule	Rule specification
Rule 1: Share financial intelligence data • Grants police investigators access to John Doe's financial intelligence data • Does not grant police investigators access to records that, if shared, could jeopardize the police investigation	A police investigator may access records in the financial intelligence system that have the following GBAC classification: ✓ **Jurisdiction** = Federal ✓ **Collection authority** = Proceeds of Crime & Terrorist Financing Act ✓ **Collection reason** = Suspicious financial transactions ✓ **Security designation** = Protected B And with the following additional criteria: ✓ **Subject name** = John Doe
Rule 2: Share investigative data • Grants intelligence analysts access to the appropriate police investigative data on John Doe • Does not grant intelligence analysts access to records that, if shared, may be potentially injurious to John Doe, such as the Protected C designation	An intelligence analyst may access records in the criminal investigation system that have the following GBAC classification: ✓ **Jurisdiction** = Federal ✓ **Collection authority** = Federal Police Act ✓ **Collection reason** = Money-laundering investigation ✓ **Security designation** = Protected B And with the following additional criteria: ✓ **Subject name** = John Doe

While the example clearly demonstrates how GBAC can improve information sharing, there are additional benefits that organizations can achieve. GBAC also allows for the seamless delivery of an organization's programs and services and enables transparency and accountability within and across organizations and jurisdictions.

GBAC rule	Rule specification
Rule 3: Share transaction data • Grants police investigators access to data on all John Doe banking transactions • Does not grant police investigators access to all cash deposit records that, if shared, would compromise clients' privacy rights; only John Doe's records are shared	The police investigator is granted access to records in the retail banking system that have the following GBAC classification: ✓ **Jurisdiction** = Federal ✓ **Collection authority** = Proceeds of Crime & Terrorist Financing Act ✓ **Collection reason** = Suspicious financial transactions ✓ **Security designation** = Protected B And with the following additional criteria: ✓ **Subject name** = John Doe
Rule 4: Share transaction data • Grants intelligence analysts access to data on all large cash deposit transactions including ones made by John Doe • Does not grant intelligence analysts access to all cash deposit records that, if shared, may compromise the clients' privacy rights; only those deposits greater than $10K, as required by legislation, are shared	The police investigator is granted access to records in the retail banking system that have the following GBAC classification: ✓ **Jurisdiction** = Federal ✓ **Collection authority** = Proceeds of Crime & Terrorist Financing Act ✓ **Collection reason** = Suspicious financial transactions ✓ **Disclosure authority** = PIPEDA ✓ **Security designation** = Protected B And with the following additional criteria: ✓ **Transaction type** = Cash deposit ✓ **Deposit amount** = › $10K

Once the GBAC rules have been agreed upon, they can be incorporated into the access control models of each organization and used to regulate access to information systems. Since the GBAC rule specifications are based upon the governance of each information asset to be accessed, access control modules can be designed and built to provide rightful access to internal and external users who have a valid need-to-know status and with whom this information can be shared.

The benefits of GBAC

Improved information sharing that manages and mitigates risks

The above scenario illustrates how GBAC can enable organizations to overcome the very real challenges of today's information-rich and privacy-concerned environment. GBAC can realize maximum information sharing benefits while managing and mitigating information sharing risks.

By classifying information according to governance and specifying the correct rules of governance, an organization can share an information asset properly, even though it does not necessarily know the intended recipients or the asset's eventual intended use. And it can share that information in a way that is consistent with relevant security, privacy and legislative principles, even though it is not always able to observe or infer the specific contents of the asset.

By mapping an information asset back to its original and governing legislation, GBAC enables an organization to easily comply with current and future legislative requirements on the sharing and protection of information. Putting in place explicit GBAC rules institutes a very strong risk management and mitigation scheme once an organization decides to share information beyond its boundaries. As described in this paper, GBAC defines the legal uses and access permission rules that must be associated with any information asset.

Improved service delivery

GBAC is not limited to enabling information sharing. A similar scenario exists for the seamless delivery of an organization's programs and services. Also referred to as a shared service delivery model, the concept is simple: citizens and customers can visit one location—whether in person, online or via telephone—and view the entire organization as a single entity.

However, many of the risks related to developing this shared service delivery model are similar in nature to what has been outlined in the information-sharing scenario: privacy, security and compliance risks. These risks have been a major barrier to developing a shared service delivery model. Due to the similarity in the nature of the risks, GBAC can be used as part of the solution, and can be employed as a key enabler to eliminate redundancies and increase overall integrity, efficiency and effectiveness. Therefore, just as GBAC enables compliant information sharing, it can be used to improve service delivery across organizations.

Improved transparency and accountability

Finally, what may be regarded as the most important benefit of GBAC is how it can better enable transparency and accountability within and across organizations and jurisdictions. With GBAC in place, each access request is associated with a GBAC rule that evaluates whether an information asset can be accessed. This access request, along with its context, can be recorded in an audit log that details who made the request (the individual user who has been assigned a role) and what was requested (the information asset granted access via the GBAC rule). If, for some reason, an audit or an investigation is required, the information contained within these logs may be used to determine who accessed the information, why it was accessed and whether the request was done in accordance with the proper governance. This information may then be used to further an investigation or may be collected as evidence. Thus, GBAC becomes a very powerful mechanism to drive transparency and accountability down to the level of each individual and to each information asset within an organization.

The challenges ahead

By no means is GBAC the complete solution. Rather, it is a critical part of the solutions required by information sharing, service delivery and improved accountability and transparency. As new systems are being built—and old systems are being retrofitted to deal with the open, interconnected, and inter-jurisdictional reality—GBAC will become a fundamental building block in any architecture where governance must be taken into account.

Implementing GBAC is not without its challenges. Big steps are ahead for organizations wishing to deploy GBAC. One of the biggest steps is simply taking the time to inventory what information holdings are in place and what legislative measures govern their use. But in the long run, GBAC will provide a sounder, simpler, more efficient and, ultimately, more cost-effective approach to managing access to information assets. When weighed against the potential costs, risks and loss of trust, implementing GBAC becomes a compelling value proposition for all organizations that share information.

GBAC can become the foundation of an organization's information sharing strategy, providing them with the following benefits:

- *Allows information to be shared across organizational boundaries and jurisdictions*
- *Provides confidence in fully complying with the law*
- *Protects the interests and privacy of all affected parties*
- *Mitigates the organization's potential risk of noncompliance and legal liability*

Conclusion

Access control methodologies have not kept pace with the technology and societal changes that have occurred over the last several years. The growing ubiquitous nature of the Internet and the increasing use of personal data requires that information must be protected according to a growing spate of legislative measures. E-government, public–private collaboration, the terrorism threat and the increasing technology available to reengineer systems and business processes are driving the trend toward sharing information across organizational and jurisdictional boundaries.

Organizations that want to comply with the seemingly conflicting requirements of sharing and protecting information are finding it impossible to do so with traditional access control models because they have no way of knowing whether they are breaking the law, wrongfully disclosing information or exposing themselves to potential liability. GBAC is a necessary approach if organizations wish to share information, while maintaining accountability and properly managing the risks associated with information sharing. GBAC solves the fundamental challenge that every organization is faced with today: How do you get the right information to the right people for the right purpose without knowing the specific details of the information?

Based on the rapid adoption of service-oriented and collaborative architectures that are fundamentally open and interoperable in nature, it is imperative that organizations protect and share information according to governing legislation as they interact with an increasingly wide array of individuals, organizations and governments.

The final conclusion is straightforward: GBAC is necessary for any organization—government, commercial or non-profit—that collects and shares information and that wishes to comply with its governing legislation, regulations and resulting policies. By making GBAC the foundation of their information sharing strategy, organizations can share information across organizational boundaries and jurisdictions, knowing that they are complying fully with the law, protecting the interests and privacy of all affected parties and mitigating their own potential risk of noncompliance and legal liability.

About CGI

Founded in 1976, CGI is a world-class leader in information technology and business process services. Through our focused industry expertise in financial services, government, healthcare, telecommunications, utilities, manufacturing, retail and distribution, we offer end-to-end services, including systems integration, strategic consulting, business solutions and the full management of IT and business functions.

Backed by rich heritage, global scale and a strong financial position, CGI has a solid track record of on-time, on-budget delivery and high-value repeat performance. Rooted in quality and management processes, our goal is to fully meet client objectives, serving as an accountable, flexible and objective partner.

To explore this topic and how we can help, contact your CGI account manager or visit www.cgi.com/web/en/head_office.htm for the location of the CGI office nearest you. Other information about CGI can be found at www.cgi.com.